PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-110193
(43)Date of publication of application : 23.04.1999

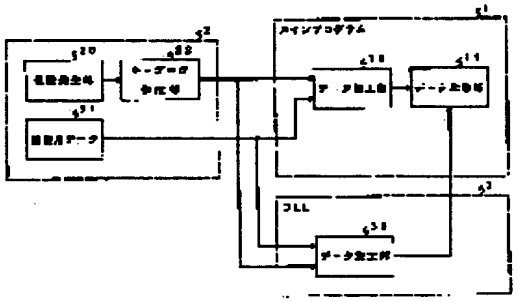
(51)Int.Cl. G06F 9/06

(21)Application number : 09-265882
(22)Date of filing : 30.09.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : TAKAHASHI MASAKI

(54) COMPUTER SYSTEM AND LIBRARY LINK METHOD APPLIED TO THE COMPUTER SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To realize a link function with a normal library by means of a library authentication function, and accordingly, to prevent forgery of library.
SOLUTION: In the computer system having a DLL(dynamic link library) function, a main program 1 inputs the authentication data and the key data to a data processing part 10 from a data generation part 2 included in an authentication function and also gives these two data to a data processing part 30 included in the authentication function of a DLL 3. A data comparison part 11 of the program 1 compares the 1st and 2nd processing data obtained from both parts 10 and 30 with each other. When both processing data are coincident with each other, the DLL 3 is authenticated as a normal library.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－110193

(43)公開日　平成11年(1999)４月23日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　9/06	４１０	Ｇ０６Ｆ　9/06	４１０Ｅ

審査請求　未請求　請求項の数９　ＯＬ　（全６頁）

(21)出願番号　特願平9－265882

(22)出願日　平成９年(1997)９月30日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　高橋　正樹
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

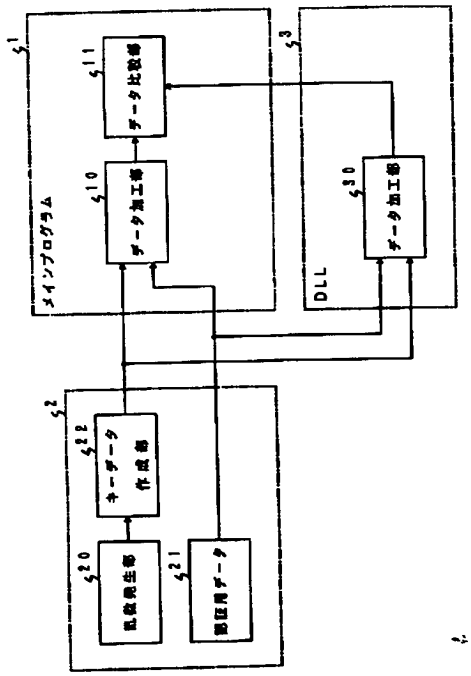
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　コンピュータシステム及び同システムに適用するライブラリのリンク方法

(57)【要約】

【課題】ライブラリに対する認証機能により正規のライブラリとのリンク機能を実現して、結果的にライブラリの偽造防止を図ることにある。

【解決手段】ダイナミック・リンク・ライブラリ機能を有するコンピュータシステムにおいて、メインプログラム１は認証用関数に含まれるデータ生成部２から認証用データとキーデータをデータ加工部１０に入力すると共に、ＤＬＬ３の認証用関数に含まれるデータ加工部３０に同一の認証用データとキーデータを与える。メインプログラム１側のデータ比較部１１は、各データ加工部１０，３０から得られた第１と第２の加工処理データとを比較し、一致した場合にＤＬＬ３を正規のライブラリとして認証する。



1

【特許請求の範囲】

【請求項１】　実行対象のプログラムと予め用意されたライブラリとをリンク処理するためのリンク機能を有するコンピュータシステムであって、

リンク対象のライブラリを認証するための認証用データを生成するための生成手段と、

前記認証用データを当該プログラム及び当該ライブラリのそれぞれに設定するための設定手段と、

当該プログラムと当該ライブラリとのリンク処理時に、当該プログラムに設定した認証用データと当該ライブラリに設定した認証用データとを比較して、比較結果が一致した場合には当該ライブラリが当該プログラムのリンク対象のライブラリであることを認証する認証手段とを具備したことを特徴とするコンピュータシステム。

【請求項２】　実行対象のプログラムと予め用意されたライブラリとのリンク処理するためのリンク機能を有するコンピュータシステムであって、

リンク対象のライブラリを認証するための認証用データ及び前記認証用データをデータ加工処理するためのキーデータを生成するための生成手段と、

前記認証用データ及び前記キーデータを当該プログラム及び当該ライブラリのそれぞれに設定するための設定手段と、

当該プログラムに設定された前記キーデータに従って前記認証用データをデータ加工処理するための第１のデータ加工手段と、

当該ライブラリに設定された前記キーデータに従って前記認証用データをデータ加工処理するための第２のデータ加工手段と、

当該プログラムと当該ライブラリとのリンク処理時に、前記第１のデータ加工手段により得られた加工処理データと前記第２のデータ加工手段により得られた加工処理データとを比較して、比較結果が一致した場合にはリンク対象のライブラリであることを認証する認証手段とを具備したことを特徴とするコンピュータシステム。

【請求項３】　前記ライブラリはダイナミック・リンク・ライブラリであり、

前記リンク機能はプログラムの実行時に当該プログラムと前記ライブラリとを動的にリンク処理することを特徴とする請求項１または請求項２記載のコンピュータシステム。

【請求項４】　前記ライブラリはダイナミック・リンク・ライブラリであり、

前記リンク機能は、前記認証手段により認証された当該ライブラリと当該プログラムとを動的にリンク処理し、前記認証手段により認証されない場合には所定のエラー処理を実行する手段を有することを特徴とする請求項１または請求項２記載のコンピュータシステム。

【請求項５】　前記生成手段は、前記リンク機能を含むプログラム制御を実行するためのシステム制御手段に含

2

まれていることを特徴とする請求項１または請求項２記載のコンピュータシステム。

【請求項６】　前記生成手段、前記設定手段、前記第１のデータ加工手段及び前記認証手段は当該プログラムにより呼出し可能な特定関数からなり、

前記第２のデータ加工手段は当該ライブラリに含まれる特定関数からなることを特徴とする請求項２記載のコンピュータシステム。

【請求項７】　実行対象のプログラムと予め用意されたライブラリとのリンク処理するためのリンク機能を有するコンピュータシステムに適用するライブラリのリンク方法であって、

リンク対象のライブラリを認証するための認証用データ及び前記認証用データをデータ加工処理するためのキーデータを生成するステップと、

前記認証用データ及び前記キーデータを当該プログラム及び当該ライブラリのそれぞれに設定するステップと、

当該プログラムに設定された前記キーデータに従って前記認証用データをデータ加工処理して第１の加工処理データを生成するステップと、

当該ライブラリに設定された前記キーデータに従って前記認証用データをデータ加工処理して第２の加工処理データを生成するステップと、

当該プログラムと当該ライブラリとのリンク処理時に、前記第１の加工処理データと前記第２の加工処理データとを比較して、比較結果が一致した場合にはク対象のライブラリであることを認証するステップと、

認証された当該ライブラリと当該プログラムとを動的にリンク処理するステップとからなることを特徴とするライブラリのリンク方法。

【請求項８】　実行対象のプログラムと予め用意されたライブラリとのリンク処理するためのリンク機能を有するコンピュータシステムにより読取り可能な記憶媒体であって、

リンク対象のライブラリを認証するための認証用データ及び前記認証用データをデータ加工処理するためのキーデータを生成するステップと、

前記認証用データ及び前記キーデータを当該プログラム及び当該ライブラリのそれぞれに設定するステップと、

当該プログラムに設定された前記キーデータに従って前記認証用データをデータ加工処理して第１の加工処理データを生成するステップと、

当該ライブラリに設定された前記キーデータに従って前記認証用データをデータ加工処理して第２の加工処理データを生成するステップと、

当該プログラムと当該ライブラリとのリンク処理時に、前記第１の加工処理データと前記第２の加工処理データとを比較して、比較結果が一致した場合にはク対象のライブラリであることを認証するステップと、

認証された当該ライブラリと当該プログラムとを動的に

リンク処理するステップとを前記コンピュータシステムが実行するように設定されたプログラムを記憶した記憶媒体。

【請求項９】　認証用データ及び前記キーデータを生成するためのステップ、前記認証用データ及び前記キーデータを当該プログラム及び当該ライブラリのそれぞれに設定するステップ、前記第１の加工処理データを生成するステップおよび前記認証するステップはそれぞれ当該プログラムにより呼出し可能な特定関数により実行される処理であり、

前記第２の加工処理データを生成するステップは当該ライブラリに含まれる特定関数により実行される処理であることを特徴とする請求項８記載の記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、特にダイナミック・リンク・ライブラリ機能を有するコンピュータシステムに関する。

【０００２】

【従来の技術】従来、パーソナルコンピュータなどのコンピュータシステムにおいて、汎用的に利用されるルーチン（ｒｏｕｔｉｎｅ）の再利用、システム機能の拡張、またはソフトウエア開発の作業分担などの理由から、特定機能毎のプログラムをモジュール単位に開発し、一つのファイルとして設定されるライブラリと称する機能が設けられている。

【０００３】ライブラリは、例えば標準的なサブルーチン群を構成する複数のオブジェクト・モジュール（メンバ）がコンパイルされて、一つのファイルとしてパッケージされたものである。システムは、通常ではリンカにより実行対象のプログラム（以下ライブラリのプログラム群と区別するためにメインプログラムと呼ぶ）とライブラリとをリンクして実行する。

【０００４】ここで、ライブラリは、スタティック・リンク・ライブラリとダイナミック・リンク・ライブラリ（以下ＤＬＬと呼ぶ場合がある）とに大別される。前者はプログラムの実行前にリンクされるライブラリであり、後者はプログラムの実行時に動的にリンクされるライブラリである。特に、ＤＬＬは、複数のメインプログラムの共有ライブラリとして機能させることができるなどの利点を備えている。

【０００５】

【発明が解決しようとする課題】ダイナミック・リンク・ライブラリ（ＤＬＬ）は、複数のメインプログラムが実行中に同じライブラリを共有できるなどの利点がある。しかしながら、そのようなＤＬＬを利用するシステムでは、例えば第三者が呼出し規則の等しいＤＬＬを偽造した場合に、メインプログラムであるアプリケーション・プログラムは想定している機能とは異なる機能のライブラリとリンクして、本来の仕様とは異なったプログラムとして動作する可能性がある。

【０００６】このため、特にセキュリティ確保に関係するＤＬＬが偽造された場合に、パスワードなどの機密情報の漏洩、プログラムやデータのコピー防止機能の解除（著作権の侵害を招く）、またはプログラムの暴走などによるシステム破壊などが発生する可能性がある。

【０００７】そこで、本発明の目的は、ライブラリに対する認証機能により正規のライブラリとのリンク機能を実現して、結果的にライブラリの偽造防止を図ることにある。

【０００８】

【課題を解決するための手段】本発明は、特にダイナミック・リンク・ライブラリ機能を有するコンピュータシステムにおいて、リンク対象のライブラリを認証するための認証用データを生成するための生成手段と、認証用データをメインプログラム（アプリケーション・プログラム）及び当該ライブラリのそれぞれに設定するための設定手段と、当該認証用データに基づいて当該ライブラリが正規のリンク対象のライブラリであることを認証する認証手段とを有するシステムである。

【０００９】具体的には、当該メインプログラム及び当該ライブラリはそれぞれ、予め用意された認証用関数（特定機能ルーチン）を呼出し、認証用データの生成処理、認証用データの設定処理、及び認証処理を実行する。当該メインプログラムでは、認証用関数が生成した認証データとリンク対象の当該ライブラリからの認証データとを比較し、比較結果が一致であれば正規のライブラリとして認証する。この認証結果に基づいて、当該メインプログラムと当該ライブラリとのリンク処理が実行される。このような方式により、仮に偽造されたライブラリが設定されている場合に、前記の認証処理によりメインプログラムに対するリンク対象ライブラリから偽造ライブラリを除去することが可能となる。

【００１０】本発明の別の観点として、リンク対象のライブラリを認証するための認証用データ及び認証用データをデータ加工処理するためのキーデータを生成するための生成手段と、認証用データ及びキーデータを当該プログラム及び当該ライブラリのそれぞれに設定するための設定手段と、当該プログラムに設定されたキーデータに従って認証用データをデータ加工処理するための第１のデータ加工手段と、当該ライブラリに設定されたキーデータに従って認証用データをデータ加工処理するための第２のデータ加工手段と、第１のデータ加工手段により得られた加工処理データと第２のデータ加工手段により得られた加工処理データとを比較して、比較結果が一致した場合にはリンク対象のライブラリであることを認証する認証手段とを有するシステムである。

【００１１】このようなシステムであれば、認証用データはキーデータに基づいて暗号化処理に相当するデータ加工処理される。従って、仮に認証用データが第三者に

5

漏洩されても、認証手段は認証用データそのものではなく、データ加工処理により得られた加工処理データに基づいて認証処理を実行するため、第三者に対するセキュリティを確保することができる。

【００１２】

【発明の実施の形態】以下図面を参照して本発明の実施の形態を説明する。図１は本実施形態に関係するシステムの概念を示すブロック図であり、図２は同実施形態に関係するリンク処理を説明するための概念図であり、図３は同実施形態に関係するコンピュータシステムのハードウェア構成を示すブロック図であり、図４は同実施形態のリンク処理を説明するためのフローチャートである。

（システム構成）本実施形態は、アプリケーション・プログラムであるメインプログラム１が実行時に、予め用意されたダイナミック・リンク・ライブラリ（ＤＬＬ）３と動的にリンクする機能を有するコンピュータシステムを想定する。

【００１３】メインプログラム１とＤＬＬ３はそれぞれ、予め用意された認証用関数（特定機能ルーチン）を呼出して実行させる機能を有する。メインプログラム１側の認証用関数は、図１に示すように、認証用データとキーデータを生成するためのデータ生成部２、データ加工部１０及びデータ比較部１１の各機能に大別する。データ生成部２は、認証データを生成する認証データ生成部２１とキーデータ作成部２２とを有する。キーデータ作成部２２は、乱数発生部２０により生成される乱数データに基づいて、予め設定された認証データを加工処理（暗号化処理）するためのキーデータを作成する。

【００１４】データ加工部１０は、キーデータ作成部２２からのキーデータに基づいて、所定のアルゴリズムにより認証データ生成部２１からの認証データを加工処理（暗号化処理）する。一方、ＤＬＬ３側の認証用関数は、メインプログラム１側と同一機能のデータ加工部３０を有する。データ生成部２は、メインプログラム１側のデータ加工部１０と同一の認証データとキーデータを与える。ＤＬＬ３側のデータ加工部３０は、データ加工部１０と同様に、キーデータに基づいて所定のアルゴリズムにより認証データを加工処理（暗号化処理）する。

【００１５】データ比較部１１は、データ加工部１０により得られる加工処理データ（暗号化された認証データであり、以下第１の加工処理データと呼ぶ）とＤＬＬ３側のデータ加工部３０により得られる加工処理データ（以下第２の加工処理データと呼ぶ）とを比較し、比較結果が一致の場合にメインプログラム１とＤＬＬ３とをリンクさせるリンク処理を実行させる。

【００１６】ここで、コンピュータシステムのハードウェア構成としては、図３に示すように、ＣＰＵ４０と、メインメモリ４１と、外部記憶装置４２と、システムバス４３とを有する例えばパーソナルコンピュータを想定する。メインメモリ４１には、メインプログラム１、ＤＬＬ３、ＯＳ（オペレーティングシステム）、及びリンカなどのソフトウエアツールがロードされる。ＣＰＵ４０は、メインメモリ４１に格納されたメインプログラム１を実行し、かつリンクされたＤＬＬ３を実行する。外部記憶装置４２は、メインプログラム１、ＤＬＬ３、ＯＳ（オペレーティングシステム）、及びリンカなどのソフトウエアツールをファイルとして保存するためのファイル装置である。

6

（本実施形態のリンク処理）以下図１と図２、及び図４のフローチャートを参照して本実施形態のリンク処理について説明する。

【００１７】まず、通常ではアプリケーション・プログラムであるメインプログラム１が実行時にＤＬＬ３にリンクする場合には、リンカ（ダイナミック・リンカ）に制御を移す。即ち、図２に示すように、リンカ１００はリンク情報に基づいて、メインプログラム１とＤＬＬ３とをリンクさせる。このリンク処理が終了すると、メインプログラム１に制御が移行して、メインプログラム１はリンクしたＤＬＬ３のプログラムモジュール（特定機能のサブルーチンなど）と共に、所定のデータ処理を実行する。

【００１８】このようなリンク機能の実行前に、本実施形態のメインプログラム１は認証用関数を呼出し、データ生成部２により認証用データとキーデータの生成処理を実行させる（ステップＳ１，Ｓ２）。さらに、メインプログラム１はＤＬＬ３の認証用関数を呼出し、当該関数に含まれるデータ加工部３０に認証用データとキーデータとを与える（ステップＳ３）。

【００１９】メインプログラム１側のデータ加工部１０は、キーデータに基づいて所定のアルゴリズムにより認証データを加工処理して、第１の加工処理データ（暗号化データ）を生成する（ステップＳ４）。一方、ＤＬＬ３側のデータ加工部３０も、キーデータに基づいて所定のアルゴリズムにより認証データを加工処理して、第２の加工処理データを生成する。

【００２０】データ比較部１１は、データ加工部１０により得られる第１の加工処理データとＤＬＬ３側のデータ加工部３０により得られる第２の加工処理データとを比較し、比較結果が一致の場合にはＤＬＬ３を正規のＤＬＬとして認証する（ステップＳ５，Ｓ６）。データ比較部１１は、ＤＬＬ３を正規のＤＬＬとして認証した場合には、前記のようにメインプログラム１とＤＬＬ３とをリンクさせるリンク処理を実行させる（ステップＳ７，図２を参照）。ここで、データ比較部１１は、比較結果が不一致の場合には、所定のエラー処理を実行させる（ステップＳ６のＮＯ，Ｓ８）。即ち、メインプログラム１はＤＬＬ３とのリンク処理が不可となる。

【００２１】以上のように本実施形態によれば、あるアプリケーション・プログラムであるメインプログラム１

7

が、実行時にＤＬＬ３と動的にリンクする場合に、予め用意された認証用関数により、リンク対象のＤＬＬ３が正規のＤＬＬであるか否かを認証する。この場合、正規のＤＬＬには、認証用関数としてデータ加工部３０が設けられて、このデータ加工部３０にはメインプログラム１のデータ加工部１０と同一の認証データとキーデータとが与えられる。

【００２２】ここで、認証用関数であるデータ加工部３０を機密にすることにより、仮に第三者が偽造したＤＬＬがシステムに設定されている場合に、この偽造ＤＬＬには認証用関数であるデータ加工部３０が設けられていない。従って、メインプログラム１がリンク対象として偽造ＤＤＬが設定されても、メインプログラム１側のデータ比較部１１は偽造ＤＤＬからは前記の第２の加工処理データが得られないため認証不可となる。このため、偽造ＤＤＬはリンク対象からは除かれることになる。換言すれば、リンク対象ライブラリから偽造ライブラリを除去できるため、メインプログラム１は常に正規のＤＬＬとリンクし、必要な特定機能ルーチンを実行することができる。

【００２３】なお、本実施形態において、データ生成部２は、メインプログラム１により呼出される認証用関数として説明したが、これに限る事なく、システムのＯＳの機能として動作してもよい。

【００２４】

【発明の効果】以上詳述したように本発明によれば、ダイナミック・リンク・ライブラリ機能を有するコンピュータシステムにおいて、ライブラリに対する認証機能を実現することにより、常に正規のライブラリとのリンク処理を行なうことができる。従って、例えば第三者が呼

8

出し規則の等しいＤＬＬを偽造した場合でも、その偽造ＤＬＬをリンク対象から外すことができる。これにより、アプリケーション・プログラムは常に想定している機能のライブラリとリンクして、必要な仕様を満足するプログラムとして動作することができる。

【図面の簡単な説明】

【図１】本発明の実施形態に関係するコンピュータシステムの概念を示すブロック図。

【図２】同実施形態に関係するリンク処理を説明するための概念図。

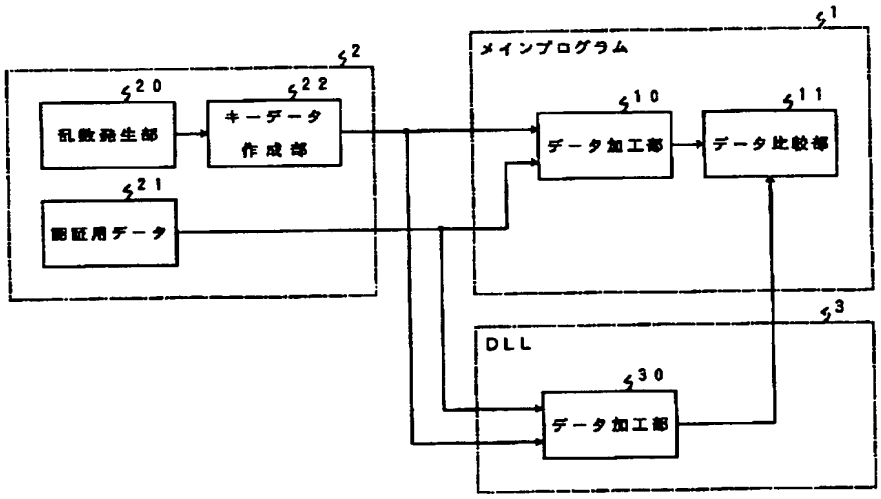
【図３】同実施形態に関係するコンピュータシステムのハードウェア構成を示すブロック図。

【図４】同実施形態のリンク処理を説明するためのフローチャート。

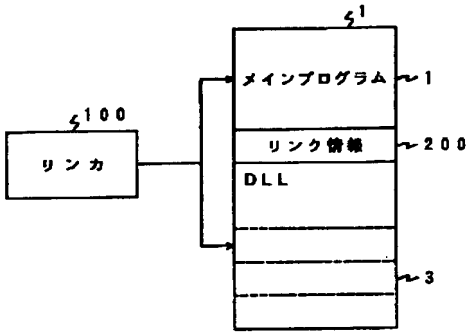
【符号の説明】

１…メインプログラム（アプリケーション・プログラム）
２…データ生成部
３…ダイナミック・リンク・ライブラリ（ＤＬＬ）
１０…データ加工部（第１のデータ加工手段）
１１…データ比較部
２０…乱数発生部
２１…認証用データ生成部
２２…キーデータ作成部
３０…データ加工部（第２のデータ加工手段）
４０…ＣＰＵ
４１…メインメモリ
４２…外部記憶装置
４３…システムバス

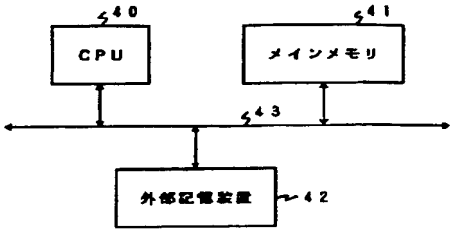
【図１】



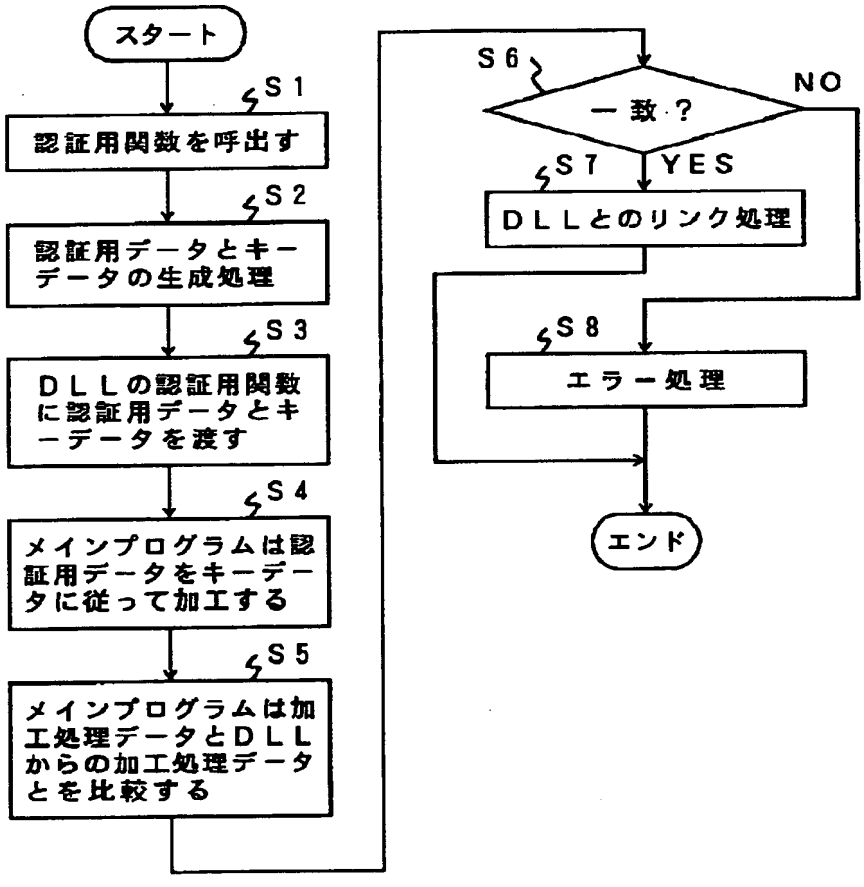
【図２】


1
メインプログラム
1
100
リンカ
リンク情報
200
DLL
3

【図３】


40
CPU
41
メインメモリ
43
外部記憶装置
42

【図４】


スタート
S1
認証用関数を呼出す
S2
認証用データとキーデータの生成処理
S3
ＤＬＬの認証用関数に認証用データとキーデータを渡す
S4
メインプログラムは認証用データをキーデータに従って加工する
S5
メインプログラムは加工処理データとＤＬＬからの加工処理データとを比較する
S6
一致？
NO
YES
S7
ＤＬＬとのリンク処理
S8
エラー処理
エンド